"(A) all available forms of such assistance,

"(B) any specific criteria which must be met to qualify for each type of assistance that is available, and

"(C) any limitations which apply to each type of assistance.

"(3) Offers of assistance under this section shall—account for—

"(A) the location of and travel time to—

"(i) the applicant's place of business; and

"(ii) schools which the applicant or members of the applicant's family who reside with the applicant attend;

"(B) the applicant's need for access to—

"(i) the site of a home or place of business whose destruction or damage is the result of the major disaster which created the applicant's need for assistance under this section: and

"(ii) crops or livestock which the applicant tends in the course of any involvement in farming which provides 25 percent or more of the applicant's annual income; and

"(C) the applicant's desire to remain in the same community.

"(4) An offer of assistance under this section shall remain available for acceptance for 60 days after the date on which such offer is made.

"(5)(A) If an applicant's eligibility for assistance is withdrawn after two offers of assistance have been made to such applicant, or if an offer of assistance is withdrawn after the 60 day period referred to in paragraph (4)—

"(i) the applicant shall, upon request, be granted a hearing to show cause why such eligibility for assistance of offer of assistance should not be withdrawn;

"(ii) the procedures for such hearing shall be the same as those which apply in a hearing to dispute a proposed termination of or eviction from temporary housing assistance and shall be fully explained to the applicant; and

"(iii) the applicant shall be given assistance in preparing for and presenting arguments at such hearing.

"(B) A final determination on any withdrawal of eligibility or an offer of assistance shall be made within ten working days after the date on which a hearing is requested under this paragraph."

SEC. 5. INCREASE IN AMOUNTS OF INDIVIDUAL AND FAMILY GRANTS.

Section 408(b) of section 601 of the Disaster Relief Act of 1974 (Public Law 93-188; 42 U.S.C. 5121 et seq.) is amended by striking "$5,000" and inserting "$7,500".

PROCESS IN CERTAIN GRANTS OF ASSISTANCE

Subsection (a) of section 601 of the Disaster Relief Act of 1974 is amended—

(1) by inserting "(1)" after "(a)", and

(2) by adding at the end the following new paragraph:

"(2) Rules and regulations authorized by paragraph (1) shall provide that payment of any assistance under this Act to a State or local government or to an eligible non-profit organization shall be completed within 60 days after the date on which an applicant submits a claim after completion of the approved work.●

● Mr. FORD. Mr. President, I wish I could say that I am pleased to join my friend from Pennsylvania in sponsoring these two bills, but I cannot. The reason for my displeasure is that there should be no need for such legislation. If there were only one role for the Federal Government after providing for the national defense, it should be disaster assistance to the States. But the Federal Emergency Management Agency—created to come to the rescue of the States in time of catastrophe—wants to cut back drastically on the assistance it provides. That is shameful.

So, you see why I take no pleasure in sponsoring this legislation. It is introduced only to prevent FEMA from making a serious mistake. The Agency's proposed rule would be devastating to Kentucky, Pennsylvania, Illinois, Indiana, Ohio, Michigan, and Wisconsin. However, I also suspect it would be just as harmful to States of the Midwest and the Great Plains, which regularly are hit by tornados—to California, which is hit by mudslides and brushfires every year—to the Gulf and Atlantic Coast States regularly lying in the path of hurricanes.

In fact, Mr. President, if the legislation we are introducing today is not signed into law before FEMA's proposed rule becomes final, every State in the Union will run the risk of being unable to respond adequately if hit by a natural disaster. I commend the Senator from Pennsylvania [Mr. HEINZ], for recognizing the potential danger of FEMA's rule, and for taking action to prevent it; and I hope my colleagues will join us in this effort.●

● Mr. LAUTENBERG. Mr. President, I am pleased to join today with my colleague from Pennsylvania, Senator Heinz, in introducing legislation to retain current Federal Emergency Management Agency policy on disaster relief.

In May, the Federal Emergency Management Agency issued draft regulations on disaster relief which, unless Congress intervenes, will become effective in October. The purpose of these regulations is to save FEMA money. The impact of the regulations is to make many communities suffering natural disasters ineligible for Federal assistance.

Mr. President, of the last 111 Presidential declarations of disasters, only 61 would be eligible for assistance under the new FEMA rules. Those found eligible for assistance would find themselves called upon to cover a far higher percentage of the cleanup and rehabilitation costs. FEMA would establish a scale of ability to pay based on per capita income. The fairness of such a sliding scale is worthy of debate and should, if it is to be implemented at all, be done legislatively and not by regulation.

To provide an example of the impact of these new regulations in New Jersey, I asked my State Office of Emergency Management to compare the cost to communities devastated by the 1984 spring floods. Passaic County, NJ had $1,664,000 in damages. After the Presidential declaration of disaster, the Federal Government paid $1,247,000 with the local match being $416,000. Under the new regulations, the local share would be $1,013,000, with FEMA covering $650,000.

Mr. President, historically, natural disasters have not been considered to be the fault of local communities and the Federal Government has attempted to quickly provide emergency relief. Until recently, the Federal Government covered 100 percent of disaster relief costs. In order to control costs, FEMA, without legislative mandate, began the 75/25 percent match with localities. That practice has not proven to be burdensome in most circumstances. Now it appears that FEMA wants to shift the burden of disaster relief primarily to States and localities.

Mr. President, the bill we are introducing will, for the first time, put in statute the 75/25 percent matching requirement. The bill will prevent FEMA from imposing, by regulation, the per capita scale which would rule States and localities ineligible for relief. The bill will prevent FEMA from adopting a 50/50 percent match.

Mr. President, as ranking minority member of the Environment and Public Works Committee's Subcommittee on Regional and Community Development, I will push for hearings on this issue. Disaster relief is one of the basic functions of Government. I strongly favor efforts to reduce unnecessary Federal spending, but I do not support efforts to save money at the expense of communities devastated by floods, hurricanes, coastal storms and other natural disasters.

I am pleased to be an original cosponsor of this legislation and urge its swift consideration and adoption.●

By Mr. LEAHY (for himself and Mr. MATHIAS):

S. 2575. A bill to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes; to the Committee on the Judiciary.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Mr. LEAHY. Mr. President, today I am introducing the Electronic Communications Privacy Act with Senator MATHIAS. The need for this legislation to update our legal privacy protections and bring them in line with modern telecommunications and computer technology is clear if we consider some simple illustrations.

In the first example, two business people are discussing their company's sensitive financial data over the telephone. Unknown to them, a competitor is using a phone tap to listen in on their conversation. Across town, a police officer has a hunch that Jane Doe is involved in drug trafficking. He goes to the Post Office and tells the postal clerk that he wants to intercept, open and read Ms. Doe's mail, and then have it resealed and delivered.

We would all agree that the competitor eavesdropper's conduct is wrong and the policeman's conduct is wrong. Their conduct is also illegal.

Now let me change the scene just a little and remind my colleagues that each example is probably going on

somewhere in the United States right now.

Instead of the two business people discussing financial matters over the telephone, they use a video teleconference system which displays their data on their video screens. The same data is picked up by their competitor. Instead of going to the Post Office, the police officer goes to an electronic mail company. Ms. Doe is a user of the system and the officer asks to see all of Ms. Doe's messages.

The only real difference between the eavesdropper's and the policeman's conduct is that in the second example, traditional telephone or mail communications have been replaced by one of the great technological innovations available in America today. Many of our constituents who use those new forms of technology in their homes and in their businesses would be surprised to learn that the same conduct is not clearly illegal once the electronic component is added to the story.

The Electronic Communications Privacy Act is designed to update our law to provide a reasonable level of Federal privacy protection to these new forms of communications. It is the culmination of 2 years of hard work. I want to commend the Senator from Maryland, the chairman of the Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks for his support and his efforts in developing this legislation.

I also want to congratulate Congressman BOB KASTENMEIER and Congressman CARLOS MOORHEAD, the chairman and ranking minority member of the House Judiciary Committee's Subcommittee on Courts, Civil Liberties and the Administration of Justice. The Congressmen and their staffs saw the House Judiciary Committee unanimously pass this landmark legislation last week.

Mr. President, let me just briefly describe the limitations of current law and the development of this legislation. The Federal wiretap statute, title III of the Omnibus Crime and Safe Streets Act of 1968 is our primary law protecting the security and privacy of business and personal communications.

Eighteen years ago, when title III was written, Congress could not appreciate—or in some cases even contemplate—telecommunications and computer technology we are starting to take for granted today: electronic mail, computer-to-computer data transmissions, cellular telephones, paging devices, and video teleconferencing. Lawmakers in 1968 could not imagine the extensive use of computers for the storage and processing of information which has put a wide range of personal and business records, including health, financial, and other records, "on-line," or the ready availability of electronic hardware, including high-technology video and radio surveillance systems, making it possible for overzealous law enforcement agencies, industrial spies, and just plain snoops to intercept the personal or proprietary communications of others.

Nor could Congress envision the dramatic changes in the telephone industry which we have witnessed in the last few years. Today, a phone call can be carried by wire, microwave, or fiber optics. Even a local call may follow an interstate path. And an ordinary phone call can be transmitted in different forms—digitized voice, data or video. In addition, since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services.

When Congress enacted title III, it had in mind one kind of communication—voice—and one kind of transmission—a transmission via a common carrier analog—or regular voice—telephone network. Congress chose to cover only the "aural acquisition" of the contents of a common carrier wire communication. The Supreme Court has interpreted that language to mean that to be covered by title III, a communication must be capable of being overheard.

Title III of the Omnibus Crime and Safe Streets Act is hopelessly out of date. It applies only to interceptions of voice communications transmitted via common carrier. It does not cover data communications. It does not specify whether or how communications made using electronic pagers or the private transmissions of video signals like those used in teleconferencing are protected.

Our 2-year effort to deal with this gap between the law and technological innovation began in 1984 when I asked the Attorney General whether he believed interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap laws.

The Criminal Division of the Department of Justice replied that Federal law protects electronic communications against unauthorized acquisition only where a reasonable expectation of privacy exists. Underscoring the need for this legislation, the Department concluded: "In this rapidly developing area of communications which range from cellular nonwire telephone connections to microwave-fed computer terminals, distinctions, such as—whether there does or does not exist a reasonable expectation of privacy—are not always clear or obvious."

Hearings in the 98th Congress held by Senator MATHIAS and myself in the Senate Judiciary Committee and by Congressman KASTENMEIER in the House Judiciary Committee demonstrated the scope of these problems and the need to act. We began working with the Justice Department and many individuals, businesses, industry groups, and civil liberty groups. Those groups were concerned primarily about the need to update the law to better protect communications privacy. They also pointed out that the absence of such privacy protections may be inhibiting further technological development in this country and that enactment of such privacy protections will encourage the full use of modern computer technology available in America today.

During those discussions, two things became very clear. First, the need to address unauthorized acquisitions of information is very real. Communications companies have been faced with Government demands, unaccompanied by a warrant, for access to the messages contained in electronic mail systems. And the unwanted private intruder, whether a competitor or a malicious teenager, can do a great deal of damage before being discovered—if he or she is ever discovered. Second, encryption is not the answer. It can be broken. More importantly, the law must protect private communications from interception by others.

The product of our discussions with the Department of Justice and private groups interested in promoting communications privacy, while protecting legitimate law enforcement needs and promoting technological innovation, was S. 1667, which Senator MATHIAS and I introduced last September. Congressmen KASTENMEIER and MOORHEAD introduced identical legislation in the House.

Shortly thereafter, the Office of Technology Assessment issued its report, "Electronic Surveillance and Civil Liberties." Again, the need for this legislation was underlined. OTA concluded that a message sent by means of an electronic mail system could be intercepted and that its contents could be disclosed to an unintended snoop. The Office of Technology Assessment study also concluded that current legal protections for electronic mail are "weak, ambiguous, or nonexistent," and that "electronic mail remains legally as well as technically vulnerable to unauthorzed surveillance."

Since that time, the Subcommittee on Patents, Copyrights, and Trademarks and the House Judiciary Committee's Subcommittee on Courts, Civil Liberties, and the Administration of Justice have held extensive hearings on the legislation. During those hearings, the Department of Justice and radio hobbyists raised some concerns about the bill. Those concerns are addressed in this new version of the Electronic Communications Privacy Act we are introducing today. This is the same language that the House Judiciary Committee passed by a vote of 34 to 0 last week.

The bill will extend coverage of title III of the Omnibus Crime and Safe Streets Act beyond only voice communications to include video and data communications. It recognizes that private carriers and common carriers

perform so many of the same functions today that a distinction between privacy standards is not warranted. The bill also creates penalties for the unauthorized access of electronically stored information if that information is obtained or altered.

In order to address radio hobbyists' concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful. Under this revised Electronic Communications Privacy bill, cellular phones, private and public microwave services and voice or display pagers are protected against interception. Cordless telephones and tone-only pagers are not.

The Electronic Communications Privacy Act provides standards by which law enforcement agencies may obtain access to both electronic communications and the records of an electronic communications system. These provisions are designed to protect legitimate law enforcement needs while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers.

At the request of the Justice Department, we strengthened the current wiretap law from a law enforcement perspective. Specifically, we expanded the list of felonies for which a voice wiretap order may be issued and the list of Justice Department officials who may apply for a court order to place a wiretap. We also added a provision making it easier for law enforcement officials to deal with a target who repeatedly changes telephones to thwart interception of his communications, and created criminal penalties for those who notify a target of a wiretap in order to obstruct it.

The bill creates a statutory framework for the authorization and issuance of an order for a pen register. It also creates civil penalties for the users of electronic communications services whose rights under the bill are violated. Finally, it preserves the careful balance governing electronic surveillance for foreign intelligence and counterintelligence purposes embodied in the Foreign Intelligence Surveillance Act of 1978. And it provides a clear procedure for access to telephone toll records in counterintelligence investigations.

Mr. President, the subcommittee staff has prepared a more detailed summary of the bill. I ask unanimous consent that the summary, along with the text of the bill, be printed in the RECORD following my remarks.

From the beginning of our history, first-class mail has had the reputation of preserving privacy while promoting commerce. It is high time we updated our laws so that we can say the same about new forms of technology which are being use side by side with first-class mail. A broad coalition of businesses, industry groups, civil liberties groups, and privacy groups are asking us to do that by enacting the Electronic Communications Privacy Act. The Department of Justice also strongly supports this legislation, and I look forward to working with my colleagues to see it passed and signed into law this year.

In closing, let me just thank the staff who have worked so hard, not only in drafting a good bill, but in working together until they successfully addressed the concerns raised during the hearings. The bill now enjoys the broadest possible support and is ready for prompt passage in the House and Senate, thanks to their efforts.

There being no objection, the previously mentioned material was ordered to be printed in the RECORD, as follows:

S. 2575

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception";

(C) by striking out "as a common carrier"; and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

(B) by inserting ", electronic," after "wire".

(4) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(5) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title);

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequence allocated under part 74 that is not exclusively allocated to broadcast auxiliary service, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTION WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(2) Section 2511(2)(f) of title 18, United States Code, is amended—

(A) by inserting "or chapter 121" after "this chapter"; and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(3) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;